Identification	**Subject**	**CMS 530:** Computer Security - 8ECTS
	Department	Computer Engineering
	Program	Graduate
	Term	Fall, 2023
	Instructor	Hafiz Muhammad Azeem Akram
	E-mail:	a.akram@khazar.org
	Classroom/hours	11 Mehseti Street, AZ1096 Baku, Azerbaijan (Neftchilar campus), Classroom: N401
Prerequisites	English proficiency	
Language	English	
Compulsory/Elective	Required	
Required textbooks and course materials	***Core textbooks:*** 1. William Stallings, Lawrie Brown. Computer Security Principles and Practice, 5th Edition, Pearson; ISBN-13: 9780138091712 2. Chuck Easttom, Computer Security Fundamentals, 5th Edition, Pearson; ISBN-13: 978-0-13-798478-7	
Course Description and outline	The aim of the course is to equip students with knowledge and skills essential for protecting digital assets and infrastructure. Throughout the course, students will engage in a systematic exploration of computer security, focusing on understanding the threats and implementing basic protection systems for device, data, and network protection. Upon successful completion of this course, students should demonstrate proficiency in the following areas: • Cyberstalking, fraud, and abuse • DoS attacks • Malware • Hacking techniques • Industrial espionage in cyberspace • Encryption • Computer security technology • Security policies • Network scanning and vulnerability scanning • Cyber terrorism and information warfare • Locating information relevant to an investigation online • Forensics • Cybersecurity engineering	
Course objectives	1. To provide students with a solid foundational understanding of computer security principles, terminology, and concepts. 2. To enable students to recognize and categorize common computer security threats, including malware, social engineering, and network attacks. 3. Developing the practical skills required to implement essential protection systems. 4. To foster the ability to critically assess the potential impact of security threats on digital assets, systems, and networks. 5. To encourage critical thinking and problem-solving skills in evaluating security vulnerabilities and devising effective mitigation strategies.	
Learning outcomes	1. Demonstrate a comprehensive understanding of fundamental computer security concepts, terminologies, and principles. 2. Identify and analyze common threat types, including malware, phishing, social engineering, and denial-of-service attacks, and assess their potential impact on computer systems and networks. 3. Develop practical skills in implementing basic protection systems for devices, data, and networks, including but not limited to device hardening, data encryption, and network security configurations.	

Teaching methods	**Lecture**	x
	Group discussion	x
	Experiential exercise	x
	Lab	x
	Course paper	x
	Others	

	Methods	Date/deadlines	Percentage (%)
Evaluation	**Survey Paper**		30
	Midterm Exam		30
	Final Exam		40
	Total		100

Policy

Research Project

As an integral component of this course, students are required to write a comprehensive survey paper. This assignment serves a pivotal role in advancing their research skills, knowledge and expertise in the field of computer security.

Guidelines to follow when writing a survey paper:

1. **Choose a Narrow and Relevant Topic:** Select a specific and well-defined topic within computer security. The topic should be relevant to current research or industry trends. Avoid overly broad subjects.
2. **Conduct Thorough Research:** Begin by conducting an extensive literature review. Search for academic papers, journal articles, conference proceedings, books, and reputable online resources related to your chosen topic.
3. **Organize Your Sources:** Create a well-organized bibliography or reference list of all the sources you find. Properly cite each source in the appropriate format (e.g., APA, IEEE, ACM) as per your course or institution's guidelines.
4. **Identify Key Themes and Trends:** Analyze the literature to identify key themes, trends, and common findings or insights within your chosen topic. Pay attention to the evolution of ideas over time.
5. **Create an Outline:** Develop a clear and structured outline for your survey paper. This should include sections such as an introduction, background, literature review, discussion, and conclusion.
6. **Introduction:** Begin with an engaging introduction that outlines the importance of the chosen topic and provides context. Clearly state the objectives and scope of your survey.
7. **Background:** Provide necessary background information to ensure that readers, including those unfamiliar with the topic, can understand the context of your survey.
8. **Literature Review:** Organize the survey into subsections based on themes or subtopics within the field. For each subsection, summarize the key findings, theories, and research methods from the literature.
9. **Critical Analysis:** Critically evaluate the strengths and weaknesses of the research you've reviewed. Identify any gaps in the existing literature and discuss areas where further research is needed.
10. **Comparison and Classification:** Compare different approaches, methodologies, or solutions discussed in the literature. Classify and categorize them based on relevant criteria.
11. **Visualization:** Use tables, charts, and graphs to visually represent data, trends, or comparisons, making it easier for readers to understand complex information.
12. **Conclusion:** Summarize the main findings and contributions of your survey. Discuss the implications of the research and suggest future directions for the field.

13. References: Provide a comprehensive list of references at the end of your paper. Ensure that each source is properly cited and follows the required citation style.

14. Proofread and Edit: Carefully proofread and edit your paper for grammar, spelling, and clarity. Consider seeking feedback from peers or instructors.

15. Formatting: Paper template will be shared with the students.

16. Acknowledgments (if necessary): If you received assistance or support during your research or writing process, acknowledge it appropriately in your paper.

- **Class Preparation**
  The lecture material will focus on the major points introduced in the text. Reading the assigned chapters and having some familiarity with them before class will greatly assist your understanding of the lecture. After the lecture, you should study your notes and work relevant problems.

- **Withdrawal (pass/fail)**
  This course strictly follows grading policy of the School of Engineering and Applied Science. Thus, a student is normally expected to achieve a mark of at least 60% to pass. In case of failure, he/she will be required to repeat the course the following term or year.

- **Cheating/plagiarism**
  Cheating or other plagiarism during the Quizzes, Mid-term and Final Examinations will lead topaper cancellation. In this case, the student will automatically get zero (0), without any considerations.

- **Professional behavior guidelines**
  The students shall behave in the way to create favorable academic and professional environment during the class hours. Unauthorized discussions and unethical behavior are strictly prohibited.

- **Ethics**
  Students should not arrive late to class.
  All cell phones must be turned off and stowed away before entering class.
  Use of any electronic devices is not allowed in the classroom and violators will be punishedaccordingly.

WK	Date/Day (tentative)	Topics	Recommended Readings
1		**Introduction to Computer Security** • How Seriously Should You Take Threats to Network Security? • Identifying Types of Threats • Assessing the Likelihood of an Attack on Your Network • Basic Security Terminology • Concepts and Approaches • How Do Legal Issues Impact Network Security? • Online Security Resources	Lecture Slides Read pp. 2-27 Review questions 1-20, pp. 27-30
2		**Networks and the Internet** • Network Basics • How the Internet Works • History of the Internet • Basic Network Utilities • Other Network Devices • Advanced Network Communications Topics • Cloud Computing	Lecture Slides Read pp. 34-65 Review questions 1-25, pp. 65-69
3		**Cyber Stalking, Fraud, and Abuse** • How Internet Fraud Works • Identity Theft • Cyber Stalking • Protecting Yourself Against Cybercrime	Lecture Slides Read pp. 74-99 Review questions 1-24 pp. 99-103
4		**Denial of Service Attacks** • DoS Attacks • Illustrating an Attack • Common Tools Used for DoS Attacks • DoS Weaknesses • Specific DoS Attacks • Real-World Examples of DoS Attacks • How to Defend Against DoS Attacks	Lecture Slides Read pp. 106-123 Review questions 1-20 pp. 123-126
5		**Malware** • Viruses • Trojan Horses • The Buffer-Overflow Attack • Spyware • Other Forms of Malware • Detecting and Eliminating Viruses and Spyware	Lecture Slides Read pp. 130-159 Review questions 1-20, pp. 159-163
6		**Techniques Used by Hackers** • Basic Terminology • The Reconnaissance Phase • Actual Attacks • Malware Creation • Penetration Testing • The Dark Web	Lecture Slides Read pp. 166 -194 Review questions 1-15, pp 194-197
7		**Industrial Espionage in Cyberspace** • What Is Industrial Espionage? • Information as an Asset • Real-World Examples of Industrial Espionage • How Does Espionage Occur? • Protecting Against Industrial Espionage • Trade Secrets • The Industrial Espionage Act • Spear Phishing	Lecture Slides Read pp. 200-220 Review questions 1-15, pp. 220-223

8		**Midterm Exam**	
9		**Encryption** • Cryptography Basics • History of Encryption • Modern Cryptography Methods • Public Key (Asymmetric) Encryption • PGP • Legitimate Versus Fraudulent Encryption Methods • Digital Signatures • Hashing • MAC and HMAC • Steganography • Cryptanalysis • Cryptography Used on the Internet • Quantum Computing Cryptography	Lecture Slides Read pp. 226-261 Review questions 1-18, pp. 261-264
10		**Computer Security Technology** • Virus Scanners • Firewalls • Antispyware • IDSs • Digital Certificates • SSL/TLS • Virtual Private Networks • Wi-Fi Security	Lecture Slides Read pp. 268-299 Review questions 1-15, pp. 299-301 **Survey Paper:** **1st Deadline**
11		**Security Policies** • What Is a Policy? • Important Standards • Defining User Policies • Defining System Administration Policies • Security Breaches • Defining Access Control • Development Policies • Standards, Guidelines, and Procedures • Disaster Recovery • Zero Trust • Important Laws	Lecture Slides Read pp. 304-330 Review questions 1-15, pp. 330-333
12		**Network Scanning and Vulnerability Scanning** • Basics of Assessing a System • Securing Computer Systems • Scanning Your Network • Testing and Scanning Standards • Getting Professional Help	Lecture Slides Read pp. 336-369 Review questions 1-20, pp. 369-373 **Survey Paper:** **1st Revision (if required)**
13		**Network Scanning and Vulnerability Scanning** (continue)	
14		**Cyber Terrorism and Information Warfare** • Actual Cases of Cyber Terrorism • Weapons of Cyber Warfare • Economic Attacks • Military Operations Attacks • General Attacks • Supervisory Control and Data Acquisitions (SCADA) • Information Warfare • Actual Cases of Cyber Terrorism • Future Trends • Defense Against Cyber Terrorism • Terrorist Recruiting and Communication	Lecture Slides Read pp. 378-402 Review questions 1-14, pp. 402-404 **Survey Paper: 2nd Revision (if required)**

		• TOR and the Dark Web	
15		Paper Presentations Final Exam Review	
		Final Exam	

Note: This course outline is subject to change.